Appl. No. 09 / 993,218
Comm. Dated July 3rd, 2005
Reply To Office action of April 7th, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1–27 (CANCELED)

28 (NEW). A network based web content identification and control system especially for wide area networks, like the Internet, comprising:

client computer(s), which are any computers in the network;

examiner host computer(s), which are any computers in the network chosen for that purpose, and which each examine web content remotely by processing tiny sized delivered identifications of said web content locally;

wherein identification(s) of web content is delivered to an examiner host computer either before, during or after a client computer receives said web content from the network;

wherein said examiner host computer compares each of said delivered identification(s) to stored identifications of web content, and on the basis of the results of said comparison either:

(a) it is performed safety or preventive measures,
(b) and / or, said client computer and / or the user of said client computer is informed about the results of said comparison,
(c) or, no specific actions are performed;

wherein said web content comprises files, web pages, e-mail messages, e-mail message attachments or any data which a client computer can acquire from the network.

PAGE 6/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-36

29 (NEW). A network based web content identification and control system according to claim 28, comprising:

wherein a said stored identification either:

(a) belongs to a specific web content,

(b) is an identification filter,

(c) or, partly belongs to a specific web content, and partly is an identification filter.

30 (NEW). A network based web content identification and control system according to claim 28, comprising:

wherein a said delivered identification comes from said client computer, from the respective source host computer of the web content, or partly from said client computer and partly from the respective source host computer of the web content.

31 (NEW). A network based web content identification and control system according to claim 28, comprising:

wherein a said delivered identification consists of file identification information and / or data identification information;

wherein a said stored identification consists of file identification information and / or data identification information;

wherein said file identification information comprises one or more of the following properties of the web content:

(a) source URL-address or other type of address,

(b) source computer URL-address or other type of address,

(c) name,

(d) type,

(e) content type,

(f) size,

(g) creation date,

(h) version number,

(i) publisher,

PAGE 7/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-36

(j) authentication certificate,

(k) or, other properties;

wherein said data identification information comprises:

(a) a check-sum or any identification value based upon the data of the web content,

(b) and / or, a data sample picked according to a certain pattern, algorithm or other rule from the web content.

32 (NEW). A network based web content identification and control system according to claim 31, comprising:

wherein said safety or preventive measures are performed when a said delivered identification matches or resembles in certain extent any of said stored identifications.

33 (NEW). A network based web content identification and control system according to claim 32, comprising:

wherein said stored identifications belong to known virus infected web content.

34 (NEW). A network based web content identification and control system according to claim 33, comprising:

wherein said safety measures include one or more of the following:

(a) preventing the download of the examined web content to the client computer,

(b) performing a virus scan on the examined web content in the client computer or in the examiner host computer,

(c) destroying the examined web content.

35 (NEW). A network based web content identification and control system according to claim 34, comprising:

wherein the examiner host computer calculates an estimate for the security threat level of the examined web content and informs it to the client computer or the user of the client computer.

PAGE 8/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-36

36 (NEW). A network based web content identification and control system according to claim 33, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification(s) is delivered to the examiner host computer by a said intermediate computer.

37 (NEW). A network based web content identification and control system according to claim 36, comprising:

wherein said safety measures include one or more of the following:

(a) the intermediate computer preventing the download of the examined web content to the client computer,
(b) the intermediate computer performing a virus scan on the examined web content,
(c) the intermediate computer destroying the examined web content.

38 (NEW). A network based web content identification and control system according to claim 36, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,
(b) a server of the internet service provider,
(c) or, a network node computer.

39 (NEW). A network based web content identification and control system according to claim 32, comprising:

wherein said stored identifications belong to known non-wanted web content.

PAGE 9/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-36

40 (NEW). A network based web content identification and control system according to claim 39, comprising:

wherein said preventive measures include preventing the download of the examined web content to the client computer, and / or destroying the examined web content.

41 (NEW). A network based web content identification and control system according to claim 39, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification(s) is delivered to the examiner host computer by a said intermediate computer.

42 (NEW). A network based web content identification and control system according to claim 41, comprising:

wherein said preventive measures include the intermediate computer preventing the download of the examined web content to the client computer, and / or the intermediate computer destroying the examined web content.

43 (NEW). A network based web content identification and control system according to claim 41, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,
(b) a server of the internet service provider,
(c) or, a network node computer.

44 (NEW). A network based web content identification and control system according to claim 28, comprising:

wherein said client computers are host computers into which data is uploaded.

PAGE 10/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-38

45 (NEW). A network based download information system especially for wide area networks, like the Internet, comprising:

client computer(s);

a host computer which keeps database of the identifications of the web content which the client computers or the users of client computers have downloaded from the network;

wherein said host computer retains client-specific information about one or more of the following:

(a) old and / or newly detected virus infections,
(b) old and / or newly detected security threats,
(c) old and / or newly determined security risk ratings,
(d) personal download statistics,

for said downloaded web content;

wherein the host computer informs / alerts the respective client computer and / or the user of said client computer, when said host computer retained client-specific information changes in certain way;

wherein a client computer and / or the user of said client computer is optionally able to access said host computer retained client-specific information;

wherein said web content comprises files or any data which a client computer can acquire from the network.

46 (NEW). A network based download information system according to claim 45, comprising:

wherein the client computer destroys the host computer appointed harmful web content and / or performs a virus scan.

PAGE 11/11 * RCVD AT 7/3/2005 10:19:32 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:Loukas * DURATION (mm-ss):07-36